NORTH DAKOTA

HOMELAND SECURITY

ANTI-TERRORISM SUMMARY

North Dakota State and Local Intelligence Center

NDSLIC

1-866-885-8295

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

The Anti-Terrorism Summary is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

QUICK LINKS

North Dakota

Nothing Significant to Report

Regional

(Montana) **Security concerns after break-in at Helena water treatment plant.** Officials are investigating a break-in at the Helena Water Treatment Facility in Montana September 15 that left more than $50,000 in damages. Authorities assured the public that the water supply was not tampered with and is safe for consumption. Source: http://www.kxlf.com/news/security-concerns-after-break-in-at-helena-water-treatment-plant/

National

Nothing Significant to Report

International

Kenyan police vow to 'finish and punish' Westgate Mall terrorists. Nairobi, Kenya (CNN) -- Several gunmen remain inside a besieged mall in Nairobi, Kenya, two senior officials said, as a deadly standoff between Kenyan forces and terrorists stretches into a fourth day. Source: http://www.cnn.com/2013/09/23/world/africa/kenya-mall-attack/index.html

Banking and Finance Industry

FBI warning users about Beta Bot malware. The FBI warned users about a campaign using the Beta Bot trojan to target online payment systems and financial institutions, as well as blocking users' access to security Web sites and disabling antivirus programs. The malware has been seen propagating via Skype and USB thumb drives Source: http://threatpost.com/fbi-warning-users-about-beta-bot-malware

Crooks hijack retirement funds via SSA portal. The Social Security Administration (SSA) and financial institutions reported a rise in identity theft cases where criminals register an account on the SSA Web portal in the name of a retiree and then divert the benefits to themselves in the form of prepaid debit cards. Source: http://krebsonsecurity.com/2013/09/crooks-hijack-retirement-funds-via-ssa-portal/

New wave of Shylock trojan targets bank customers. Researchers at Zscaler warned of a new campaign using the Shylock (also known as Caphaw) trojan to target financial institutions. The initial infection vector is currently unknown but thought to be an exploit kit targeting Java vulnerabilities. Source: http://www.net-security.org/malware_news.php?id=2592

U.S. indicts ex-traders in JPMorgan 'London Whale' scandal. Two former traders for JPMorgan Chase & Co. were indicted by a U.S. grand jury for their alleged role in a $6.2 billion trading loss.

The two, a Spanish national and a French national, allegedly inflated the value of securities to hide the extent of their losses. Source: http://www.reuters.com/article/2013/09/16/us-jpmorgan-whale-indictment-idUSBRE98F13K20130916

SEC charges 23 firms with short selling violations in crackdown on potential manipulation in advance of stock offerings. The U.S. Securities and Exchange Commission announced enforcement actions against 23 firms for short selling violations, with 22 of the companies reaching settlements that totaled $14.4 million in fines. Source: http://www.sec.gov/News/PressRelease/Detail/PressRelease/1370539804376

Chemical and Hazardous Materials Sector

Nothing Significant to Report

Commercial Facilities

Refer to the ***International*** section for related information

Communications Sector

Nothing Significant to Report

Critical Manufacturing

2003-'04 Honda Odyssey and 2003 Acura MDX recalled for airbag problem. Honda announced a recall of about 374,000 model year 2003-2004 Honda Odyssey and 2003 Acura MDX vehicles due to electrical issues that could lead to inadvertent airbag deployment. Source: http://www.edmunds.com/car-news/2003-2004-honda-odyssey-and-2003-acura-mdx-recalled-for-airbag-problem.html

Waterlogic recalls about 48,000 water dispensers due to potential fire risk. Waterlogic issued a recall for about 48,000 water dispensers due to an issue with the hot water tank that can cause it to stop functioning, cause the machine to overheat, and potentially cause a fire. Source: http://www.wxyz.com/dpp/money/consumer/recalls/waterlogic-recalls-about-48000-water-dispensers-due-to-potential-fire-risk

Feds recall nearly 200,000 Suzuki models for airbag defect. Suzuki announced a recall of about 200,000 model year 2006-2011 Grand Vitara and model year 2007-2011 SX4 vehicles due to a faulty airbag sensor that could cause the front passenger airbag to deploy in a crash regardless of whether an adult or child is in the seat. Source: http://www.latimes.com/business/autos/la-fi-hy-autos-suzuki-recall-airbag-20130916,0,3871226.story

Defense/ Industry Base Sector

Nothing Significant to Report

Emergency Services

Nothing Significant to Report

Energy

Energy sector companies targeted in watering hole attack, Cisco warns. Researchers at Cisco identified a watering hole cyberattack campaign targeting energy sector companies in various parts of the world, a supplier company to nuclear and aerospace companies, and financial services companies that specialize in the energy sector. Ten Web sites were compromised by iframe injection and use iframes to load exploit code and malware taking advantage of vulnerabilities in Java, Internet Explorer, Firefox, and Thunderbird. Source: http://news.softpedia.com/news/Energy-Sector-Companies-Targeted-in-Watering-Hole-Attack-Cisco-Warns-384511.shtml

Energy Department spends $30M to bolster utility cybersecurity tools. The U.S. Department of Energy awarded 11 security vendors $30 million September 19 to develop technology the agency believes will better protect the nation's electric grid and oil and gas infrastructure from cyberattacks. Source: http://www.networkworld.com/news/2013/091913-energy-department-cybersecurity-274005.html

Halliburton pleads guilty to destruction of evidence regarding oil spill. Halliburton pleaded guilty in United States federal court September 19 to criminal charges that it destroyed evidence related to the 2010 BP Gulf oil spill and received a $200,000 penalty and probation period of 3 years. Source: http://richmond.legalexaminer.com/toxic-substances/halliburton-pleads-guilty-to-destruction-of-evidence-regarding-gulf-oil-spill/

Food and Agriculture

Nothing Significant to Report

Government Sector (including Schools and Universities)

(New York) **Federal government to seize NYC skyscraper tied to Iran.** The U.S. Department of Justice announced that it was granted a judgment allowing it to seize an office building in New York City because the company that owns the building is allegedly a front company for a front company for the Iranian government, and that the company engaged in money laundering and violations of sanctions. Source:

http://www.usatoday.com/story/news/nation/2013/09/17/fifth-avenue-skyscraper-iran-government-seizure/2829517/

Information Technology and Telecommunications

Hackers bypass iPhone 5S Touch ID. Members of the Chaos Computer Club (CCC) found a way to defeat the Touch ID biometrics mechanism on Apple iPhone 5S models by using a high-resolution picture of a user's fingerprint and then making a latex mold of the fingerprint. Source: http://threatpost.com/hackers-bypass-iphone-5s-touch-id

New file encrypting ransomware CryptoLocker targets organizations. Emsisoft researchers discovered a new family of ransomware dubbed CryptoLock (or Trojan:Win32/Crilock) which encrypts files important to businesses with AES encryption and demands a ransom to decrypt them. The ransomware appears to be targeting businesses due to the types of files it encrypts and the types of emails used to distribute its downloader. Source: http://news.softpedia.com/news/New-File-Encrypting-Ransomware-CryptoLocker-Targets-Organizations-384790.shtml

New virus protects itself by freezing hard disk. Researchers at Bkav discovered a new rootkit that creates a restore point of sorts that prevents users from making modifications to the hard disk to remove the virus. Source: http://news.softpedia.com/news/New-Virus-Protects-Itself-by-Freezing-Hard-Disk-384132.shtml

Researchers create undetectable layout-level hardware trojans. A group of researchers published a paper outlining how hardware trojans could be implemented stealthily below the gate level. The trojans can weaken protection in random number generators, create a method for leaking secret keys, and when tested were not detected by common trojan testing methods. Source: http://www.net-security.org/secworld.php?id=15589

Too long passwords can DoS some servers. A vulnerability in popular open source Web application framework Django was demonstrated where an attacker could create an extremely long password, which Django would then hash with the PBKDF2 algorithm, tying up system resources. Large passwords being repeatedly submitted could thus be used in a denial of service (DoS) attack. Source: http://www.net-security.org/secworld.php?id=15591

Experts analyze operations of state-sponsored cybercriminals behind the Bit9 hack. Symantec researchers analyzed the attacks and campaigns of a state-sponsored cybercriminal group dubbed Hidden Lynx and found that it was split into two teams utilizing two trojans to steal information through various means. The group, that is apparently China-based, was behind an attack on Bit9 in 2012, and has predominantly targeted organizations in the U.S. Source: http://news.softpedia.com/news/Experts-Analyze-Operations-of-State-Sponsored-Cybercriminals-Behind-the-Bit9-Hack-383796.shtml

National Monuments and Icons

Nothing Significant to Report

Postal and Shipping

Nothing Significant to Report

Public Health

(Massachusetts) **Bomb threats called into 5 CVS stores in Boston.** Police are searching for a suspect who called in bomb threats to 5 CVS stores around Boston September 20. No devices were found after officers searched the pharmacies. Source: http://www.boston.com/metrodesk/2013/09/20/bomb-threats-called-into-cvs-pharmacies-boston/qq4EniHZM3Y6RGu8AlpvyJ/story.html

Pharmacy bomb threats reported across Utah, nation. Authorities responded to a series of bomb threats at Walmart and Walgreens stores nationwide September 18 in which the caller demanded that several prepaid cards be loaded with money and numbers read aloud over the phone. A number of stores were evacuated and searched but no explosive devices were found. Source: http://www.deseretnews.com/article/865586639/Pharmacy-bomb-threats-reported-across-Utah-nation.html

U.S. seeing worst measles outbreak in 15 years. The U.S. Centers for Disease Control and Prevention released a report stating 2013 has had a high number of measles cases so far, and is shaping up to be one of the worst years for the disease in nearly 15 years. Source: http://www.nj.com/news/index.ssf/2013/09/us_seeing_worst_measles_outbreak_in_15_years.html

3 germs are urgent threats to USA's health, CDC says. The U.S. Centers for Disease Control and Prevention released a report September 16 claiming that the overuse of antibiotics has caused 3 kinds of bacteria to become urgent threats to human health in the U.S. The report is the first to categorize the threats in order of immediate importance and it is also the first to quantify the impact, stating the bacteria cause at least 2 million infections and 23,000 deaths a year. Source: http://www.usatoday.com/story/news/nation/2013/09/16/cdc-germ-list/2819577/

Transportation

U.S. orders 3,800 Honeywell aircraft beacons inspected. The Federal Aviation Administration ordered airlines to inspect more than 3,800 planes equipped with Honeywell emergency beacons to check for damage after a fire on an Ethiopian Airlines Boeing 787 was likely caused by a beacon. Source: http://www.reuters.com/article/2013/09/17/us-faa-honeywell-idUSBRE98G1CN20130917

Water and Dams

Refer to the ***Regional*** section for related information, item # 1

(Louisiana) **Deadly brain amoeba in tap water may be tied to Katrina.** The St. Bernard Parish school system shut off water fountains and used chlorine to kill off a deadly parasite found in the water system to get the water back up to a safe standard after a brain-eating amoeba killed a boy while he was playing outdoors. Source: http://www.nbcnews.com/health/deadly-brain-amoeba-drinking-water-may-be-tied-katrina-4B11186085

Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168